UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,939	04/19/2005	Franciscus Lucas Kamperman	NL 021063	4488

24737 7590 03/05/2010
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/05/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/531,939
Filing Date: April 19, 2005
Appellant(s): KAMPERMAN ET AL.

Robert M. McDermott
Reg. 41,508
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/23/2009 appealing from the Office action mailed 07/20/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

WO 01/76294 A1	Jonsson	11-2001
2002/0157002 A1	Messerges et al.	10-2002
7,020,781 B1	Saw et al.	3-2006
5,204,897	Wyman	4-1993
WO 01/18628 A2	Moskowitz et al.	3-2001
6,135,646	Kahn et al.	10-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-3, 5, 6, 8-10, 12, 13 and 31 are rejected under 35 U.S.C. 102(b) as being anticipated by Jonsson (WO 01/76294 A1).

With respect to claim 1, Jonsson discloses the limitation of "authorizing an operation on a machine requested by a first user on a content item comprising:

receiving, at the machine, a user right certificate (authority profile; page 3, lines 30-33) that identifies a second user and authorizes the second user to perform the requested operation on the content item, and authorizing the operation on the machine by the first user upon receipt of information from the first user (page. 7, lines 27-35 and page. 9, lines 3-20) that links the first user and the second user as members of a common authorized domain (client structure; page 3, lines 27-30)" as a first user in a first client structure is provided with the ability to give a second user (page 2, lines 30-43) assigned to a second client structure authority to access said first client structure (page. 9, lines 3-20). It is further noted that both users are registered with the access provider (page 4, lines 14-18) and users in client structures are provided access to services where service is defined as any type of information or object which may be accessible or subject to manipulation (page 3, lines 17-19). Figure 5 details how authority profiles are maintained thus linking users to a common authorized domain.

With respect to claim 2, Jonsson discloses the limitation of "the information comprises one or more domain certificates identifying the first and second users as members of the authorized domain" (page 2, lines 24-31) as a client structure, associated with a service provider, includes a number of associated services made available by the access provider and at least one assigned user. Further more, Jonsson (page 8, lines 20-25) states that when a user in a client structure wishes to use or order a certain service, he sends a signal from his home page to the access provider server that determines the specific service provider. Examiner interprets the described

client structure to be equivalent to the domain comprising of users connected by predetermined relationships. Therefore, when the access provider determines if a user and a service provider belong to the same client structure, it is equivalent to determining if a user and a service provider belong to the same domain.

With respect to claim 3, Jonsson teaches that all users have authority profile which links them to services of a service provider [domain; pg. 3, lines 17-30].

With respect to claim 5, Jonsson discloses the limitation of "the operation comprises at least one of: a rendering of the content item, a recording of the content item, a transfer of the content item and a creation of a copy of the content item" (page 7, lines 11-14) as a super-user in this client structure will assign the new employee thereto, with access to said piece of information. The level of authority will e.g. include "reading, but not revising."

With respect to claim 6, Jonsson teaches receiving a content right containing necessary information for performing the requested operation on the content item, the user right certificate of the second user authorizing the second user to perform the requested operation using the content right (pg. 9, lines 10-20).

With respect to claim 8, it is rejected in view of the same reasons as stated in the rejection of claim 1.

With respect to claim 9, it is rejected in view of the same reasons as stated in the rejection of claim 2.

With respect to claim 10, it is rejected in view of the same reasons as stated in the rejection of claim 3.

As per claim 12, Jonsson teaches receiving an identifier for the first user from an identification device and to perform the operation if the received identifier matches the identification of the first user in the user right of the first user (pg. 9, lines 10-20).

With respect to claim 13, it is rejected in view of the same reasons as stated in the rejection of claim 6.

As per claim 31, Jonsson teaches receiving a content right containing necessary information for performing the requested operation on the content item, the user right certificate of the second user authorizing the second user to perform the requested operation using the content right (page 7, lines 27-35).

Claims 4 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jonsson (WO 01/76294 A1).

With respect to claim 4, Jonsson is silent in disclosing one or more domain certificates comprise a single certificate identifying the first and second users as members of the authorized domain. Jonsson does teach both users names on a single certificate (figure 5, table 2). Jonsson also teaches multiple certificates to store the rights of the users for the domain (figure 5). One of ordinary skill would have known that all of the information could have been stored on a single certificate. Therefore, the claims are obvious because one of ordinary skill in the art could have modified the teachings of Jonsson and stored all of the users on a single certificate.

With respect to claim 11, it is rejected in view of the same reasons as stated in the rejection of claim 4.

Claims 7 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jonsson (WO 01/76294) view of Messerges et al. (US Publication 2002/0157002 A1).

With respect to claim 7, it is noted that Jonsson does not specifically disclose the limitation of "the operation is not authorized if the content right does not identify the authorized domain." However, Messerges discloses the above mentioned limitation

(page 9, paragraph 0080) because only registered devices are allowed access to the content, a check-in/check-out policy is not needed and a user's experience is greatly simplified and enhanced. Security is encountered by an end-user only when adding new devices to one or more domains. Since the devices are registered with a domain, it is understood that a device not registered with a domain will be denied access to the content. It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Messerges into the system of Jonsson to provide security because the devices that are not members of the authorized domain are prevented from access to the digital content.

With respect to claim 21, it is rejected in view of the same reasons as stated in the rejection of claim 7.

Claims 14 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jonsson (WO 01/76294 A1) in view of Saw et al. (US Patent 7,020,781 B1).

With respect to claim 14, Jonsson is silent in explicitly teaches at least a portion of the content right is encrypted using an encryption key for which a corresponding decryption key is available to the device. Saw discloses the limitation of "at least a portion of the content right is encrypted using an encryption key for which a corresponding decryption key is available to the device" (column 5, lines 47-50) as the initialization request may also include a session symmetric key that can be used to

encrypt and decrypt data packets to be sent during the transfer of the digital content. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use encryption to increase the protection of the content in Jonsson.

With respect to claim 32, Jonsson is silent in disclosing extracting a public key from the content right and to use the extracted public key in determining whether the operation is authorized. Saw teaches this above limitation (col. 3, lines 24-28). It is well known in the art to use public/private key cryptography. Substituting known equivalent technologies which process predictable results is obvious to one of ordinary skill in the art.

Claims 15-17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jonsson (WO 01/76294) in view of Wyman (US Patent 5,204,897).

With respect to claim 15, it is noted that Jonsson does not specifically disclose the limitation of "the content right is provided with a digital signature allowing verification of the authenticity of the content right." However, Wyman discloses the abovementioned limitation (column 14, lines 50-53) as the decoding algorithm using a public key for any signatures is thus used by the license server or delegatee to make sure a product use authorization is authentic. It would have been obvious to one of the ordinary skill in the

art at the time of the invention to incorporate teachings of Wyman into the system of Jonsson because that would further improve the security of the digital content.

With respect to claims 16, 17, and 19, Examiner supplies the same rationale for combining the digital signatures of Wyman into the system of Jonsson. The use of a public key in a certificate is then required to check the signature. This is inherent in the art of cryptography.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jonsson (WO 01/76294) and Wyman (US Patent 5,204,897) and in further view of Moskowitz et al. (WO 01/18628 A2).

With respect to claim 18, it is noted that neither Jonsson nor Wyman disclose the limitation of "refuse to perform the operation if the digital signature cannot be verified successfully using a digital certificate associated with an authorized content provider and a digital watermark associated with the authorized content provider is present in the content item." However, Moskowitz discloses (page 3, lines 19-21) that the digital data set may be embedded with at least one robust open watermark, which permits the content to be authenticated. It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Moskowitz into the system of Jonsson and Wyman to improve the security of the digital content through the use of

watermarks which are intended to prevent or deter unauthorized copying of digital media.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jonsson (WO 01/76294) in view of Kahn et al (US Patent 6,135,646).

With respect to claim 20, it is noted that Jonsson does not specifically disclose the limitation of "determining a robust fingerprint for the content item and to refuse to perform the operation if the determined robust fingerprint does not match a robust fingerprint comprised in the content right." However, Kahn discloses the abovementioned limitation (column 6, line 65 – column 7, line 3) as retaining a copy of the properties record for each digital object, a digital signature or other "fingerprint" of the digital object (the digital signature and other fingerprint is typically considerably smaller than the object itself) suitable for verification purposes and a temporal history list of related objects. It would have been obvious to combine teachings of Kahn into the system of Jonsson to provide improved protection for multimedia from unauthorized redistribution.

(10) Response to Argument

Group #1: Claims 1-3, 5-6, 8-10, 12-13, and 31.

With respect to Appellant's argument of group #1 of the Appeal Brief, the Examiner respectfully disagrees and refers Appellant to the rejections above as well as the detailed discussion set forth below.

Issue #1:

With respect to the independent claims 1 and 8, Examiner maintains that the recited limitations are taught by Jonsson (WO 01/76294). Appellant alleges that Jonsson fails to teach **(i)** "receiving a user right certificate that authorizes a second user to perform an operation requested by a first user", and fails to teach **(ii)** "authorizing the operation by the first user upon receipt of information that links the first user and the second user as members of a common authorized domain".

With respect to **(i),** Appellant contends that Jonsson fails to teach a user right certificate. On the surface, the "authority profile" in Jonsson is not named "user right certificate". However, upon closer inspection it can be seen that Jonsson's "authority profile" provides equivalent functionality to the "user right certificate". Jonsson does in fact teach an authority profile which defines the level of authority with which certain

services can be accessible by a user associated to said authority profile (page 3, lines 30-32). It is evident from Jonsson's invention that this authority profile grants a user's rights to services. Thus it is found to be equivalent to the claimed user right certificate.

Now turning to the embodiment on page 9 of Jonsson, there are two users involved. They will be referred to as the controlling user (first user) and the requesting user (second user). This is to avoid confusion with the two users of the claims which are referred to in the opposite fashion. However it is clear that in the claims the controlling user is the second user and the requesting user is referred to as the first user. Jonsson teaches that the controlling user gives to the requesting user access to services of his client structure. The client structures are defined by Jonsson (page 3, lines 27-29) as an entity that is associated with a number of services made available for a client, and a number of users having certain access to a subset of said services. The client structure is therefore, equivalent to a domain. A domain is a collection of services or devices to which users can be made members. Membership affords users permission to services based on their user rights which can be expressed by authority profiles. Jonsson teaches that each client structure has a superuser (controlling user) which has the entire set of rights for the client structure. Superusers can then assign rights to other users in that particular client structure (page 5, lines 10-22). Superusers are afforded this right because their authority profile has the highest level of authority. Once a superuser identifies himself as the superuser of his/her domain, the act of assigning another user to said domain can proceed. Back to the embodiment on page 9, we see this taking place whereby the controlling user gives the requesting user

access to the controlling user's client structure. The machine/server must have access to the controlling user's authority profile for authentication purposes. The identified controlling client can then create an authority profile of his client structure for the requesting user as evident by the fact that he defines which services the requesting user will have access to.

The claimed invention does not support more than is shown in this above mentioned embodiment. The claim does not define where the user right certificate originates or when it is received at the machine. Jonsson clearly teaches receiving a user right certificate [authority profile of the controlling user] that authorizes a second user [controlling user; superuser] to perform an operation requested by a first user [requesting user].

With respect to **(ii)**, in the same embodiment as recited above, the requesting user is authorized once the username is provided to log into the homepage. The username is important because the controlling user had to type in that piece of information to identify the requesting user. The authority profiles are shown with the user's names in Figure 5. Moreover, the authority profile now includes the name of the requesting user linked to his/her services. Once identified, the controlling user created the authority profile which affords the requesting user permission to services on the controlling user's client structure. Thus the requesting user is now an authorized member of the same domain as the controlling member. When the requesting user signs in, he/she has a new reference to the controlling user's domain and the allocated

services. By the reference, the requesting user may perform an operation on content because he/she has been authorized to do so by the controlling user.

Issue #2:

With respect to claim 2 and similar claim 9, Appellant has alleged that Jonsson does not teach that the information provided by the requesting user comprises one or more domain certificates identifying the first and second users as members of the authorized domain. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As shown above in the embodiment on page 9, the information of the requesting user is linked by his/her authority profile which has been created by the controlling user. This authority profile is not only linked to the requesting user but also to the client structure of the controlling user. Jonsson explicitly states new users are associated to the new client structure (pg. 9, line 5), thus they were not already in a common authorized domain. But once the controlling user has created an authority profile for the requesting user, the requesting user is identified as a member of the controlling user's client structure. The domain certificates as recited in claim 2 are not afforded the narrow scope which is argued on page 7 of the appeal brief.

Appellant argues that that the certificate is issued by a trusted third party and that it is transportable. In response to appellant's argument that the references fail to show

certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., trusted third party and a **transportable** certificate) are not recited in the rejected claim(s). There is neither a claimed trusted third party nor does the claim require transporting the certificate. Thus, the claim is not interpreted as such. Absent a third party, the domain certificate could have originated from the controlling user. The authority profile created for the requesting user is found to be equivalent to the domain certificate as claimed, because it certifies the requesting user to the controlling user's domain (client structure). If this interpretation is not proper, Jonsson also teaches that a server of the access provider in the client structure can associate an authority profile for a client when new services are requested commensurate with the permissions to access said new service (pg. 8, lines 10-15).

After further consideration of the claimed invention and the Jonsson reference, it is evident that claimed features are anticipated by Jonsson. Appellant's arguments are not persuasive in pointing out differences between the claimed invention and that of the prior art.

Group #2: Claims 4, 7, 11, 14-17, 19, 21, and 32

With respect to Appellant's argument of group #2 of the Appeal Brief, the Examiner respectfully disagrees and refers Appellant to the rejections above as well as the detailed discussion set forth below. Examiner maintains that Jonsson teaches all of the limitations of the parent claims from which claims 4, 7, 11, 14-17, 19, 21, and 32

depend. As such, Examiner maintains that these cited references under 35 U.S.C. 103(a) render group #2 unpatentable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael Vaughan

/MICHAEL R VAUGHAN/

Examiner, Art Unit 2431

Conferees:

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2431